506,908

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. September 2003 (25.09.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/079609 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32, G07B 17/00

(21) Internationales Aktenzeichen: PCT/DE03/00760

(22) Internationales Anmeldedatum:
10. März 2003 (10.03.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 11 265.7 13. März 2002 (13.03.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE POST AG** [DE/DE]; Charles-de-Gaulle-Str. 20, 53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **MEYER, Bernd** [DE/DE]; Zum Stöckerhof 2 c, 53639 Königswinter (DE). **LANG, Jürgen** [DE/DE]; Schau ins Land 15, 51429 Bergisch Gladbach (DE).

(74) Anwalt: **PATENTANWÄLTE JOSTARNDT - THUL**; Brüsseler Ring 51, 52074 Aachen (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:
— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR THE GENERATION OF CHECKABLE FORGERY-PROOF DOCUMENTS

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ERSTELLUNG PRÜFBAR FÄLSCHUNGSSICHERER DOKUMENTE

(57) Abstract: The invention relates to a method and a device for the generation of checkable forgery-proof documents with an externally supplied cryptographic module, whereby the checking of authenticity of the document is carried out without using key information belonging to the cryptographic module. According to the invention, the method and the device are characterised in that the cryptographic module is supplied with two types of data, even on supply from a communication partner which is cryptographically not trustworthy, which either remain in the cryptographic module or are attached to the document. The information remaining in the cryptographic module is used to secure the document information by means of a check value and the information transferred into the document serves to verify the securing of the document by the cryptographic module during a check of the authenticity of the document at a checkpoint.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Erstellung prüfbar fälschungssicherer elektronischer Dokumente mit einem extern gespeisten kryptografischen Modul, wobei die Prüfung der Unverfälschtheit der Dokumente ohne Benutzung von Schlüsselinformationen erfolgt, die dem kryptografischen Modul eigen sind. Erfindungsgemäß zeichnen sich das Verfahren und die Vorrichtung dadurch aus, dass das kryptografische Modul auch bei einer Speisung über kryptografisch nicht vertrauenswürdige Kommunikationspartner mit zwei Arten von Daten versorgt wird, die zum einen im kryptografischen Modul verbleiben und die zum anderen an das Dokument angehängt werden, wobei die im kryptografischen Modul verbleibenden Informationen genutzt werden, um die Dokumentinformationen über einen Prüfwert abzusichern und wobei die in das Dokument übernommenen Informationen dazu dienen, im Rahmen einer Prüfung der Unverfälschtheit des Dokuments in einer Prüfstelle die Absicherung des Dokuments durch das kryptografische Modul nachzuweisen.

WO 03/079609 A1